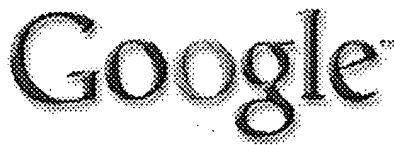


L Number	Hits	Search Text	DB	Time stamp
2	2272	380/277-286.ccls. or 380/44-45.ccls. or 380/28-30.ccls.	USPAT	2004/03/17 13:15
3	817	713/176.ccls. or 713/181.ccls. or 713/189.ccls.	USPAT	2004/03/17 13:16
4	2851	(380/277-286.ccls. or 380/44-45.ccls. or 380/28-30.ccls.) or (713/176.ccls. or 713/181.ccls. or 713/189.ccls.)	USPAT	2004/03/17 13:16
5	11	((generat\$4 near4 first near5 key near5 pair) and (asymmetric or public adj2 key)) and (message near3 recover\$4)	USPAT; EPO; JPO; DERWENT	2004/03/17 13:16
6	18	(message near3 recover\$4) same (key near4 pair)	USPAT; EPO; JPO; DERWENT	2004/03/17 13:17
7	541	(generat\$4 or creat\$4 or deriv\$5) near3 key adj3 pair	USPAT; EPO; JPO; DERWENT	2004/03/17 13:17
8	235	((generat\$4 or creat\$4 or deriv\$5) near3 key adj3 pair) and ((380/277-286.ccls. or 380/44-45.ccls. or 380/28-30.ccls.) or (713/176.ccls. or 713/181.ccls. or 713/189.ccls.))	USPAT; EPO; JPO; DERWENT	2004/03/17 13:18
9	499	second near3 key near4 pair	USPAT; EPO; JPO; DERWENT	2004/03/17 13:18
10	71	(second near3 key near4 pair) and ((380/277-286.ccls. or 380/44-45.ccls. or 380/28-30.ccls.) or (713/176.ccls. or 713/181.ccls. or 713/189.ccls.))	USPAT; EPO; JPO; DERWENT	2004/03/17 13:18
-	81	generat\$4 near4 first near5 key near5 pair	USPAT	2004/03/17 08:58
-	54940	asymmetric or public adj2 key	USPAT	2004/03/16 13:50
-	67	(generat\$4 near4 first near5 key near5 pair) and (asymmetric or public adj2 key)	USPAT	2004/03/16 13:50
-	2180	message near3 recover\$4	USPAT	2004/03/17 09:10
-	10	((generat\$4 near4 first near5 key near5 pair) and (asymmetric or public adj2 key)) and (message near3 recover\$4)	USPAT	2004/03/17 09:19
-	1	("5341425").PN.	USPAT	2004/03/17 08:58
-	1	("5270809").PN.	USPAT	2004/03/17 08:59
-	1	("5506904").PN.	USPAT	2004/03/17 09:00
-	1	("5381481").PN.	USPAT	2004/03/17 09:00
-	1	("5341425").PN.	USPAT	2004/03/17 09:01
-	1	("5200823").PN.	USPAT	2004/03/17 09:01
-	11	cain and gammie	USPAT	2004/03/17 09:03
-	1	(message near3 recover\$4) same (second near2 key near4 pair)	USPAT	2004/03/17 11:11
-	17	(message near3 recover\$4) same (key near4 pair)	USPAT	2004/03/17 13:17
-	10	((generat\$4 near4 first near5 key near5 pair) and (asymmetric or public adj2 key)) and (message near3 recover\$4)	USPAT	2004/03/17 13:16
-	4	((message near3 recover\$4) same (key near4 pair)) and (((generat\$4 near4 first near5 key near5 pair) and (asymmetric or public adj2 key)) and (message near3 recover\$4))	USPAT	2004/03/17 09:26
-	1	second near3 key near4 pair and MRA	USPAT	2004/03/17 09:27
-	2	key near4 pair and MRA	USPAT	2004/03/17 09:27

-	420	second near3 key near4 pair	USPAT	2004/03/17 13:18
-	2164	message near3 recov\$5	USPAT	2004/03/17 09:28
-	1	(second near3 key near4 pair) same (message near3 recov\$5)	USPAT	2004/03/17 09:28
-	24	(second near3 key near4 pair) and (message near3 recov\$5)	USPAT	2004/03/17 11:10


[Advanced Search](#) [Preferences](#) [Language Tools](#) [Search Tips](#)

The "AND" operator is unnecessary – we include all search terms by default.
[\[details\]](#)

[Web](#) · [Images](#) · [Groups](#) · [Directory](#) · [News](#)

Searched the web for public key and message recovery. Results 1 - 10 of about 726,000. Search took 0.40 sec

JITC Public Key Infrastructure Introduction

... only the originator's **public key** could be used to decrypt the signature into the correct **message** digest of the document. Data and **Key Recovery** Reasons for data ...

jtc.fhu.disa.mil/pki/intro.html - 16k - Mar 16, 2004 - [Cached](#) - [Similar pages](#)

[PDF] 7. Recovery of Public key file

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 2 7.1 **Recovery of Your Own Public Key File** In this ... **key** file name exists in the folder, the following **message** is displayed. ... When recovering a **public key** file by ...

www.hmi-jp.com/english/englishninja/engninja/engno7.pdf - [Similar pages](#)

[PDF] Key Recovery in SecretAgent

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Since a new data encrypting **key K** and a new ephemeral **public key** shared by O ... O needs to make a new, auditable, **key recovery** request for each **message**. ...

www.infosecorp.com/news/press/pdf/sakr.pdf - [Similar pages](#)

[PDF] Signature scheme with message recovery and its application

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... is effective in applications like **public key** certifying protocols and **key** exchange protocols ... encryption scheme using the **message recovery** signature in ...

www.isical.ac.in/~malapati_r/sig-raja.pdf - [Similar pages](#)

Course 2821: Designing and Managing a Windows Public Key ...

... manual and automatic **key** archival and **recovery** in a Windows ... Implement secure e-mail **messages** by using Microsoft ... Module 1: Overview of **Public Key Infrastructure**. ...

www.microsoft.com/traincert/syllabi/2821Afinal.asp - 63k - [Cached](#) - [Similar pages](#)

[PDF] Cryptanalysis of Nyberg-Rueppel's message recovery scheme - IEEE ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... is a permutation of and is the secret **key** corresponding to **public key** the second part of the signature and the corresponding **message recovery** equations are ...

crypto.ee.ncku.edu.tw/pdf/41.pdf - [Similar pages](#)

IEEE P1363a: Signatures with message recovery

... the third draft specifies techniques of an integrated (ie a hybrid of symmetric **key** and **public key** techniques) signature scheme with partial **message recovery**. ...

grouper.ieee.org/groups/1363/P1363a/SigMR.html - 3k - [Cached](#) - [Similar pages](#)

Key Recovery v Recovery of Keys (Was Royal Mail Viacode)

... Previous **message**: **Key Recovery v Recovery of Keys** ... Was Royal Mail Viacode); Next **message**: NSA lawsuit ... is this technically possible > with **public key** cryptography ...

www.chiark.greenend.org.uk/pipermail/ukcrypto/1999-December/007339.html - 4k - [Cached](#) - [Similar pages](#)

Why Corporate Message Recovery isn't GAK

... fear a number of people have expressed that Corporate **Message Recovery** (CMR) could be ... strength **keys** (128 bits or more), backed with a full-strength **public key**. ...

www.imc.org/ietf-openpgp/mail-archive/msg00228.html - 10k - [Cached](#) - [Similar pages](#)

Key Recovery in the CMP (RESEND WITH LINE FEEDS)

... the syntax for a new **message**, KeyRecoveryReq, be ... to specifically address the required fields for **key recovery**. ... used to supply a signature **public key** for which ...

www.imc.org/ietf-pkix/old-archive-99/msg00072.html - 8k - [Cached](#) - [Similar pages](#)

[[More results from www.imc.org](#)]

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

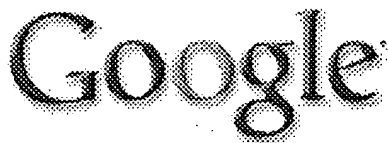
[Search within results](#)

Dissatisfied with your search results? [Help us improve.](#)

Get the [Google Toolbar](#):

[Google Home](#) - [Advertise with Us](#) - [Business Solutions](#) - [Services & Tools](#) - [Jobs, Press, & Help](#)

©2004 Google



[Advanced Search](#)
[Preferences](#)
[Language Tools](#)
[Search Tips](#)

public key and message recovery

Google Search

The "AND" operator is unnecessary – we include all search terms by default.
[\[details\]](#)

Web · Images · Groups · Directory · News ·

Searched the web for public key and message recovery. Results 11 - 20 of about 726,000. Search took 0.21 se

Citations: Message recovery for signature schemes based on the ...

... process of a partially blind threshold signature is simplified by a group **public key**. The proposed scheme provides the **message recovery** capability [13, 23]. ...

citeseer.nj.nec.com/context/59250/0 - 36k - [Cached](#) - [Similar pages](#)

Citations: Commercial Key Recovery - Walker, Lipner, Ellison ...

... CKR system[13] in that in CKR the process manufactures its own **key**, which is stored in the **message**, encrypted by the **public key** of the Data Recovery Center (DRC ...

citeseer.nj.nec.com/context/97469/0 - 12k - [Cached](#) - [Similar pages](#)

[[More results from citeseer.nj.nec.com](#)]

Cryptography Terminology

... **Key recovery** is central to the US government's new encryption policy ... the IDEA secret **key** as part of the **message**. PKAF **Public Key** Authentication Framework. ...

www.efa.org.au/Issues/Crypto/crypto5.html - 10k - [Cached](#) - [Similar pages](#)

INTERNET-DRAFT Jonathan Trostle draft-ietf-cat-kerberos-pk ...

... the **recovery** of a compromised Kerberos V5 KDC using **public key** cryptography ... data fields and error data fields in Kerberos **messages** to transport **recovery** data ...

www.ietf.org/proceedings/98dec/I-D/draft-ietf-cat-kerberos-pk-recovery-01.txt - 21k - [Cached](#) - [Similar pages](#)

INTERNET-DRAFT Jonathan Trostle draft-ietf-cat-kerberos-pk ...

... PK-RECOVERY-DATA ::= SEQUENCE { kdcPubValueld [0] INTEGER, – Copied from error – **message** kdcPublicKeyKvno [1] INTEGER OPTIONAL – New KDC **public** – **key** kvno ...

www.ietf.org/proceedings/98aug/I-D/draft-ietf-cat-kerberos-pk-recovery-00.txt - 25k - [Cached](#) - [Similar pages](#)

[[More results from www.ietf.org](#)]

Introduction to Public-Key Cryptography

... to a backup copy of the **key**, for example, the encrypted **messages** can never ... The renewal process may involve reusing the same **public-private key** pair or ...

developer.netscape.com/docs/manuals/security/pkin/contents.htm - 75k - [Cached](#) - [Similar pages](#)

Key Recovery v Recovery of Keys (Was Royal Mail Viacode)

... of **Keys** (Was Royal Mail Viacode); Next **message**: **Key Recovery** ... Two new **key** pairs are then generated, one handles ... The **public keys** are made **public**, and the private ...

www.chiark.greenend.org.uk/pipermail/ukcrypto/1999-December/007332.html - 4k - [Cached](#) - [Similar pages](#)

[[More results from www.chiark.greenend.org.uk](#)]

Commercial key recovery

... The individual user's file or **message** encryption software is ... with extensions to store the per-item **key** encrypted with the assigned or selected **public key**. ...

portal.acm.org/citation.cfm?id=227240&jmp=cit&dl=GUIDE&dl=ACM&CFID=11111111&CFTOKEN=2... - [Similar pages](#)

IEEE P1363 Research Contributions: Cryptographic Schemes and ...

... improving the security and efficiency of symmetric-**key** and **public-key** encryption ... Although

several **message recovery** schemes exist, their security is questionable ...

grouper.ieee.org/groups/1363/Research/Schemes.html - 10k - [Cached](#) - [Similar pages](#)

[[More results from grouper.ieee.org](#)]

Commercial Data Recovery

... **recovery** information with the **message** in the form of a second crypto recipient.

In addition mechanisms are provided in the form of a proposed CMR **public key** ...

www.cypherspace.org/adam/cdr/ - 19k - [Cached](#) - [Similar pages](#)



Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [Next](#)

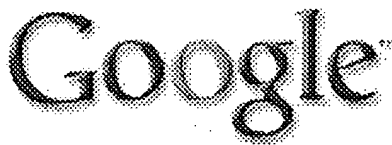
public key and message recovery

Google Search

[Search within results](#)

[Google Home](#) - [Advertise with Us](#) - [Business Solutions](#) - [Services & Tools](#) - [Jobs, Press, & Help](#)

©2004 Google



[Advanced Search](#)
[Preferences](#)
[Language Tools](#)
[Search Tips](#)

public key and message recovery

Google Search

The "AND" operator is unnecessary – we include all search terms by default.
[\[details\]](#)

Web · Images · Groups · Directory · News ·

Searched the web for public key and message recovery and key pair generator. Results 1 - 10 of about 49,40
 By default, Google searches for variations of your search terms. To search only for an exact term, place a '+' sign

[PDF] Key Recovery in SecretAgent

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... K and a new ephemeral **public key** shared by ... outputs a (signed and encrypted) **key recovery key** (KRK ... **Message Recovery Utility**: inputs an encrypted archive and ...

www.infosecorp.com/news/press/pdf/sakr.pdf - [Similar pages](#)

[PDF] Key Management and ANSI X9.44

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... responder **key pair** only? ... Digital Signature Schemes - -2,-3 Giving **Message Recovery**
 • ISO/IEC 9798-3 Entity Authentication using a **Public Key** Algorithm • ISO ...

csrc.nist.gov/encryption/kms/x944-slides.pdf - [Similar pages](#)

[PDF] Contents

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... of a Digital Signature 138 **Message Digests** 141 ... and the X.509 Standard 171 **Public-Key**
 Certificates 172 ... the Pull Model 195 Managing **Key Pairs** 196 **Generating Key** ...

www.osborne.com/networking...comm/ 007213139X/007213139X...toc.pdf - [Similar pages](#)

JITC Public Key Infrastructure Introduction

... **message**, because only the originator's **public key** could be ... the signature into the
 correct **message** digest of ... Data and **Key Recovery** Reasons for data **recovery** may ...

jitc.fhu.disa.mil/pki/intro.html - 16k - Mar 16, 2004 - [Cached](#) - [Similar pages](#)

Re: PKIX Part 3 REQUIRES SUPPORT OF KEY RECOVERY?

... This would be a **message** effectively > asserting that "the ... as occurring wherever either
 the **public** or private component of a **key pair** first occurs in a ...

www.imc.org/ietf-pkix/old-archive-97/msg00806.html - 6k - [Cached](#) - [Similar pages](#)

Re: key recovery options for PKIX-3 CAs?

... Charles, did you see my original **message**? ... with sooner or later, if only for corporate
key recovery. ... the same, regardless of where the **public key** was **generated**. ...

www.imc.org/ietf-pkix/old-archive-97/msg00865.html - 10k - [Cached](#) - [Similar pages](#)

[[More results from www.imc.org](#)]

[PPT] Some Perspectives on Smart Card Cryptography

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... **Key Pair Generation**. ... 160-320 bits overhead for signatures with **message recovery**. ... Paillier,
 "Smart Card Crypto-Coprocessors for **Public-Key** Cryptography," RSA ...

www.rsasecurity.com/rsalabs/staff/bios/bkaliski/publications/ other/kaliski-smart-card-crypto-scia-1998.ppt -

[Similar pages](#)

[PPT] Emerging Standards for Public-Key Cryptography

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... h **message recovery**. ISO9796-1 (M). Related Scheme Operations. Domain parameter
generation.

Domain parameter validation. **Key pair generation**. **Public key** validation. ...

www.rsasecurity.com/.../bkaliski/publications/emerging-standards/kaliski-emerging-standards-brics-1998.ppt - [Similar pages](#)

[[More results from www.rsasecurity.com](#)]

: Class XKMSKeyData

... Method Detail. **returningPrivateKey**. **public** boolean **returningPrivateKey()** Returns whether a private **key** will be returned in the response **message**. ...

www.xmltrustcenter.org/developer/verisign/tsik/docs/api/com/verisign/xkms/client/XKMSKeyData.html - 20k - Mar 16, 2004 - [Cached](#) - [Similar pages](#)

mySecureSign Philippines: Enterprise Trust Services

... is also encrypted, using a **public key** belonging to ... enterprise control over encryption **key-pair generation**, **key** and certificate ... send an e-mail **message** to esales ...

www.mysecuresign.com/key_management.html - 14k - [Cached](#) - [Similar pages](#)

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

[Search within results](#)

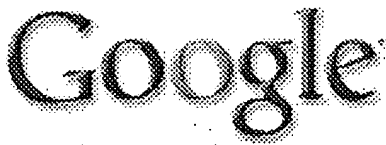
Dissatisfied with your search results? [Help us improve.](#)

Get the [Google Toolbar](#):



[Google Home](#) - [Advertise with Us](#) - [Business Solutions](#) - [Services & Tools](#) - [Jobs, Press, & Help](#)

©2004 Google


[Advanced Search](#) [Preferences](#) [Language Tools](#) [Search Tips](#)

The "AND" operator is unnecessary – we include all search terms by default.
[\[details\]](#)

[Web](#) · [Images](#) · [Groups](#) · [Directory](#) · [News](#)

Searched the web for public key and message recovery and key pair generator. Results 11 - 20 of about 49,4
 By default, Google searches for variations of your search terms. To search only for an exact term, place a '+' sign

Key Recovery v Recovery of Keys (Was Royal Mail Viacode)

... Was Royal Mail Viacode); Next **message: Key Recovery** ... get revoked and the current ((**public**)
 signature validation ... Two new **key pairs** are then **generated**, one handles ...

www.chiark.greenend.org.uk/pipermail/ ukcrypto/1999-December/007332.html - 4k - [Cached](#) - [Similar pages](#)

[PDF] Microsoft PowerPoint - chap13new

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... **public keys** signature **generation message** private **key** ... Share a symmetric **key** Share
 trusted **public keys** ... registration and destruction **key recovery** revocation **key** ...

sconce.ics.uci.edu/seminar/slides/chap13new.pdf - [Similar pages](#)

[PDF] Microsoft PowerPoint - chap13

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... **keys** (class 2) signature **generation message** private **key** ... symmetric **key** T Trusted **public**
-key T cross ... de-registration and destruction **key recovery** revocation **key** ...

sconce.ics.uci.edu/seminar/slides/chap13.pdf - [Similar pages](#)

[[More results from sconce.ics.uci.edu](#)]

VeriSign Australia: Whitepaper:Enterprise Key Management

... When a **public-private key pair** is used in protecting ... such a capability, loss of a
 private **key** may mean ... unlock encrypted files or stored e-mail **messages**, or if ...

www.verisign.com.au/whitepapers/enterprise/ management/key_mng1.shtml - 10k - [Cached](#) - [Similar pages](#)

[PDF] IEEE P1363a / D2 Standard Specifications for Public Key ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... M 10.5.3 Signature Verification (and **Recovery**) Operation (new for D2 ... by a verifier
 and the **message** M recovered ... the other party's purported **public key** w' and ...

grouper.ieee.org/groups/1363/P1363a/ contributions/PVSSR.pdf - [Similar pages](#)

An Introduction to PKI, covering pki, public key cryptography ...

... to as **key escrow** or **key recovery**.) **Public Key** ... e-mail systems headers, addresses and
 body **messages** may have ... a signed request containing their **public key** to the ...

www.articsoft.com/wp_pki_intro.htm - 27k - [Cached](#) - [Similar pages](#)

[PDF] Public Key Infrastructure

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... their own hash of the **message** Digital Signature ... Repository Certificate Revocation
Key Recovery Automatic **Key** ... Understanding **Public Key** Infrastructure Carlisle ...

www.lug.psu.edu/presentations/pki.pdf - [Similar pages](#)

Tales from the Cryptographer #2: The cost of forging digital ...

... back the signature S to the **message** M under the **public key** y corresponding to ... with
message recovery for some fake n-bit **message** M. Let Sean's **key pair** be (x ...

planeta.terra.com.br/informatica/ paulobarreto/tales2.html - 6k - [Cached](#) - [Similar pages](#)

[PDF] 1.264 Lecture 5

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... **key** encrypted with receiver's **public key**, as usual ... Session **key** encrypted with government **key recovery agency key** • **Message** – Controversy continues ...

ocw.mit.edu/.../838DA073-4757-4A35-8FAC-54E0896759B7/0/1264_lecture_17_F2002.pdf - [Similar pages](#)

House of Commons - Trade and Industry - Seventh Report

... and unforgeable identifier of the sender and the **message**. ... May be facilitated by a **key recovery** agent. ... **Public Key** Encryption, A method of encryption in which ...

www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/187/18719.htm - 13k - [Cached](#) - [Similar pages](#)



Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [Next](#)

public key and message recovery

Google Search

[Search within results](#)

[Google Home](#) - [Advertise with Us](#) - [Business Solutions](#) - [Services & Tools](#) - [Jobs, Press, & Help](#)

©2004 Google


[Advanced Search](#) [Preferences](#) [Language Tools](#) [Search Tips](#)

The "AND" operator is unnecessary – we include all search terms by default.
[\[details\]](#)

[Web](#) · [Images](#) · [Groups](#) · [Directory](#) · [News](#)

Searched the web for public key and message recovery and key pair generator. Results 21 - 30 of about 49,4
 By default, Google searches for variations of your search terms. To search only for an exact term, place a '+' sign

From: pgut001@cs.auckland.ac.nz (Peter Gutmann) To: cryptography ...

... ietf-pkix-cmmf-00.txt), PKI **message** formats, has ... of the private **key** corresponding to the **>public key** of the ... archive the private **> – key** of a **key pair** which the ...

www.scramdisk.clara.net/other/pgut_pki_new.txt - 9k - [Cached](#) - [Similar pages](#)

[RTF] IEEE P1363: Standard Specifications for Public-Key Cryptography

File Format: Rich Text Format - [View as HTML](#)

... the signer's "**public key**". (optional) validate the **public key**. ... **Key** agreement schemes (TBD). Signature schemes. DL/EC scheme with **message recovery**. ...

grouper.ieee.org/groups/1363/P1363/presentation/ P1363-Presentation-8-17-99.rtf - [Similar pages](#)

[[More results from grouper.ieee.org](#)]

Introduction to Public-Key Cryptography

... copy of the **key**, for example, the encrypted **messages** can never be ... The renewal process may involve reusing the same **public-private key pair** or issuing a ...

developer.netscape.com/docs/manuals/ security/pkin/contents.htm - 75k - [Cached](#) - [Similar pages](#)

Comgate Engineering Ltd. - Secure Messaging

... and verify the digital signature on the **message**. ... issuing certificates, and **keys** (both **public** and private **key** ... certificate revocation; **key** back-up and **recovery**; ...

www.comgate.com/smsging/smsging.htm - 14k - [Cached](#) - [Similar pages](#)

[PDF] Certificates, Certification Authorities and Public-Key ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... **Keys** – Are refreshed at each proactive **recovery** execution – Each ... Used only to sign notification **message** for the new server **public key** © Babaoglu 2003 ...

www.cs.unibo.it/babaoglu/courses/ security/lucidi/PKI.pdf - [Similar pages](#)

Crypto AG – Information + Communication Security Glossary

... a **public-key** cryptosystem, consisting of the **public key** and private ... **Key Recovery** A special feature of a **key** management scheme that allows **messages** to be ...

www.crypto.ch/pages/htm/crypto/glossary/k.htm - 29k - [Cached](#) - [Similar pages](#)

[Fwd: GESG Identity-Based Public Key Cryptography (ID-PKC)]

... DIV>> <DIV></DIV>> > ---Original **Message**---DIV></DIV>> ... The **public pair** for all these **keys** <DIV></DIV>>will be placed on a **key** list which ...

www.chiark.greenend.org.uk/pipermail/ ukcrypto/2001-August/016863.html - 12k - [Cached](#) - [Similar pages](#)

[[More results from www.chiark.greenend.org.uk](#)]

[PDF] IEEE P1363 / D8 . Standard Specifications for Public Key ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... RSA signature verification if the **public** exponent of ... potentially one byte for some **key** sizes) compared ... why are signature schemes with **message recovery** using ISO ...

www.informatik.tu-darmstadt.de/.../Artikel/Kryptographie/ PublicKeyAllgemein/P1363-C-10-05-98.pdf - [Similar pages](#)

[PDF] [White Paper Public Key Encryption and digital signature How do ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 4. **Key backup and recovery**: What happens to encrypted files ... Without **key** backup, all **messages** and files that have been encrypted with his **public-key** can no ...

www.cgi.com/cgi/pdf/cgi_whpr_35_pki_e.pdf - [Similar pages](#)

[Re: Photuris terminology](#)

... secret is used instead of a **public/private key** ... As I noted in another **message**, not revealing ... applies to authentication, encryption, and **key generation**, as well ...

www.vpnc.org/ietf-ipsec/92.ipsec/msg02335.html - 9k - [Cached](#) - [Similar pages](#)



Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [Next](#)

[public key and message recovery](#)

[Google Search](#)

[Search within results](#)

[Google Home](#) - [Advertise with Us](#) - [Business Solutions](#) - [Services & Tools](#) - [Jobs, Press, & Help](#)

©2004 Google